UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/529,778	03/30/2005	Michael A. Epstein	US020358US	2264

24737 7590 02/11/2008
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER
PACHURA, REBECCA L

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
02/11/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

D

Office Action Summary	**Application No.** 10/529,778	**Applicant(s)** EPSTEIN, MICHAEL A.	
	Examiner Rebecca L. Pachura	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 March 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5-11,13-17 and 19-21* is/are rejected.

7)☒ Claim(s) *4,12 and 18* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 March 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☒ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *03/30/2005*.
4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. **Claims 1-21 are presented for examination.**

The claims and only the claims form the metes and bounds of the invention. "Office personnel are to give claims their broadest reasonable interpretation in light of the supporting disclosure. In re Morris, 127 F.3d 1048, 1054-55, 44 USPQ2d 1023, 1027-28 (Fed. Cir. 1997). Limitations appearing in the specification but not recited in the claim are not read into the claim. In re Prater, 415 F.2d 1393, 1404-05, 162 USPQ 541, 550-551 (CCPA 1969)" (MPEP p 2100-8, c 2, l 45-48; p 2100-9, c 1, l 1-4). The Examiner has full latitude to interpret each claim in the broadest reasonable sense. The Examiner will reference prior art using terminology familiar to one of ordinary skill in the art. Such an approach is broad in concept and can be either explicit or implicit in meaning.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 03/30/2005 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Priority

3. The claim for priority from the US Provisional Application No. 60/445263 filed on 02/05/2003 is duly noted. On the Transmittal Letter submitted on 07/27/2006 a priority date of 09/30/2002 is claimed the examiner does not know what this refers to. A claim for priority from the US Provisional Application No. 60/141944 filed on 07/01/1999 is not acknowledged because it both had expired before PCT/US03/04123 was filed and it does not support any of the claims in the current application.

Change of Power of Attorney

4. The change of Power of Attorney submitted on 03/30/2005 is duly noted.

Oath/Declaration

5. The oath or declaration is defective. A new oath or declaration in compliance with 37 CFR 1.67(a) identifying this application by application number and filing date is required. See MPEP §§ 602.01 and 602.02.

The oath or declaration is defective because:

It was not executed in accordance with either 37 CFR 1.66 or 1.68. Frederic Grumiaux failed to sign the Oath/Declaration.

It does not identify the mailing address of each inventor. A mailing address is an address at which an inventor customarily receives his or her mail and may be either a home or business address. The mailing address should include the ZIP Code designation. The mailing address may be provided in an application data sheet or a supplemental oath or declaration. See 37 CFR 1.63(c) and 37 CFR 1.76.

Double Patenting

6. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In*

re Van Ornum, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1, 2, 3, 4, 6, 7, 9, 10, 11, 12 are provisionally rejected on the grounds of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 2, 3, 4, 5, 8, 9, 11, 12, 13, 14 of copending Application No. 10529353 in view of "TCP/IP Illustrated, vol. 1, The Protocols" (Stevens) (Applicant's IDS). It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that processing the time required to generate a response is another way to verify the target and its response. This is a provisional obviousness-type double patenting rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are

> such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. **Claims 1-3, 5-11, 13-17, and 19-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over "TCP/IP Illustrated, vol. 1, The Protocols" (Stevens) (Applicant's IDS) in view of US 6446028 (Wang), and in view of "Using Encryption for Authentication in Large Networks of Computers" (Needham).**

As to claim 1, Stevens discloses a method of determining proximity of a target node to a source node, comprising: communicating a query from the source node to the target node, communicating a response from the target node to the source node (Stevens page 2, paragraph 4: Historically the ping program has operated in a mode where it sends an echo request once a second, printing each echo reply that is returned). Stevens fails to teach the response from the target node including a measure of processing time required to generate the response based on the query.

However, Wang discloses the response from the target node including a measure of processing time required to generate the response based on the query (Wang abstract: A client-server software performance monitor system is disclosed. In the system of the present invention, a performance monitor machine is coupled to a computer network in close network proximity to one or more server systems that are to be monitored. The performance monitor machine monitors all network communication originating from or addressed to the server system to determine client-server transaction times. The performance monitor machine calculates a server processing time by subtracting the time when the server system receives the request packet from a client system from the time when the server system sends the first response packet back to the client system. The performance monitor machine also calculates a network transit time by subtracting said time when the server system receives the final acknowledgement packet from the time when said server system sent the first response packet to the client system. The performance monitor machine calculates an approximate total client observed response time by adding the server processing time and the approximate network transit time).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that keeping track of system processing time was a common thing to do (Wang abstract: A client-server software performance monitor system is disclosed. In the system of the present invention, a performance monitor machine is coupled to a computer network in close network proximity to one or more server systems that are to be monitored. The performance monitor machine monitors all network communication originating from or addressed to the server system to determine client-server transaction times. The performance monitor machine calculates a server processing time by subtracting the time when the server system receives the request packet from a client system from the time when the server system sends the first response packet back to the client system. The performance monitor machine also calculates a network transit time by subtracting said time when the server system receives the final acknowledgement packet from the time when said server system sent the first response packet to the client system. The performance monitor machine calculates an approximate total client observed response time by adding the server processing time and the approximate network transit time).

The modified Stevens discloses receiving the response at the source node, determining a measure of query-response time between communicating the query and receiving the response (Stevens page 2, paragraph 6 and page 3, paragraph 1: When the ICMP echo reply is returned, the sequence number is printed, followed by the TTL, and the round-trip time is calculated…ping is able to calculate the round-trip time by storing the time at which it sends the echo request in the data portion of the ICMP message), and determining the proximity of the target node based on a communication time that depends upon a difference between the measure of query-response time and the measure of processing time (Stevens page 2, paragraph 4: …these newer implementations send only a single echo request and output "host is alive" if an echo reply is received, or "no answer" if no reply is received within 20 seconds).

As to claim 2, the modified Stevens discloses the method of claim 1. The modified Stevens fails to teach wherein the query and response correspond to at least a portion of a cryptographic key-exchange protocol.

However, Needham discloses wherein the query and response correspond to at least a portion of a cryptographic key-exchange protocol (Needham page 995, column 1, paragraph 2-4 and column 2, paragraph 1: The protocol opens with A communicating in clear to AS his own claimed identity and the identity of the desired correspondent, B, together with A's nonce identifier for this transaction, I_{a1}. ("Nonce" means "used only once.") Here the nonce identifier must be different than others used by A in previous messages of the same type. The first message of the protocol is:

A --) AS: A, B, I_{AI} (1.1)

Upon receiving message (1.1), AS looks up the secret, identifying keys of both parties and also computes a new key CK that will be the key for the conversation if all goes well. The next transaction is a rather complicated message from A S to A:

AS--) A: $\{I_{A1}, B, CK, \{CK, A\}^{KB}\}^{KA}$ (1.2)

where KA and KB are A's and B's secret, identifying keys. Because (1.2) is encrypted with A's secret key, only A can decrypt it and discover the conversation key CK. Following decryption, A checks for the presence of the intended recipient's name, B, and the correct identifier, I_{A1}, in order to verify that the message really is a reply by AS to the current enquiry. Both the name of the intended recipient and the transaction identifier must appear in message (1.2). If the recipient's name is left out, then an intruder could change that name in message (1.1), say to X, before AS receives it, with the subsequent result that A would unknowingly communicate with X instead of B. If the identifier is left out, then an intruder could substitute a previously recorded message (1.2) (from AS to A about B) and force A to reuse a previous conversation key. A remembers CK and sends the part encrypted with KB to B:

A --) B: $\{CK, A\}^{KB}$ (1.3)

The real B, but no other, will be able to decrypt message (1.3) and emerge with the conversation key CK, the same as A has. B also knows the identity of the intending correspondent, as authenticated by AS.

It is worth reviewing at this point the state of knowledge of the two parties. A now knows that any communication he receives encrypted with CK must have originated with B, and also that any communication he emits with CK encryption will be understood only by B. Both are known because the only messages containing CK that have ever been sent are tied to A's and B's secret keys. B is in a similar state, mutatis mutandis. It is important, however, to be sure that no part of the protocol exchange or ensuing conversation is being replayed by an intruder from a recording of a previous conversation between A and B. In relationship to this question the positions of A and B differ. A is aware that he has not used the key CK before and therefore has

no reason to fear that material encrypted with it is other than the legitimate responses from B. B's position is not so good; unless he remembers indefinitely keys previously used by A in order to check that CK is new, he is unclear that the message (1.3) and the subsequent messages supposedly from A are not being replayed. To guard against this possibility, B generates a nonce identifier for the transaction, I_B, and sends it to A under CK:

B --) A: $\{I_B\}^{CK}$ (1.4)

expecting a related reply, say one less:

A --) B: $\{I_B - 1\}^{CK}$ (1.5)

If this reply is satisfactorily received, then the mutual confidence is sufficient to enable substantive communication, encrypted with CK, to begin.

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that this Needham-Schroeder key-exchange protocol is a cryptographic key-exchange protocol (Needham page 995, column 1, paragraph 2-4 and column 2, paragraph 1: The protocol opens with A communicating in clear to AS his own claimed identity and the identity of the desired correspondent, B, together with A's nonce identifier for this transaction, I_{a1}. ("Nonce" means "used only once.") Here the nonce identifier must be different than others used by A in previous messages of the same type. The first message of the protocol is:

A --) AS: A, B, I_{AI} (1.1)

Upon receiving message (1.1), AS looks up the secret, identifying keys of both parties and also computes a new key CK that will be the key for the conversation if all goes well. The next transaction is a rather complicated message from A S to A:

AS--) A: $\{I_{A1}, B, CK, \{CK, A\}^{KB}\}^{KA}$ (1.2)

where KA and KB are A's and B's secret, identifying keys. Because (1.2) is encrypted with A's secret key, only A can decrypt it and discover the conversation key CK. Following decryption, A checks for the presence of the intended recipient's name, B, and the correct identifier, I_{A1}, in order to verify that the message really is a reply by AS to the current enquiry. Both the name of the intended recipient and the transaction identifier must appear in message (1.2). If the recipient's name is left out, then an intruder could change that name in message (1.1), say to X, before AS receives it, with the subsequent result that A would unknowingly communicate with X instead of B. If the identifier is left out, then an intruder could substitute a previously recorded message (1.2) (from AS to A about B) and force A to reuse a previous conversation key. A remembers CK and sends the part encrypted with KB to B:

A --) B: $\{CK, A\}^{KB}$ (1.3)

The real B, but no other, will be able to decrypt message (1.3) and emerge with the conversation key CK, the same as A has. B also knows the identity of the intending correspondent, as authenticated by AS.

It is worth reviewing at this point the state of knowledge of the two parties. A now knows that any communication he receives encrypted with CK must have originated with B, and also that any communication he emits with CK encryption will be understood only by B. Both are known because the only messages containing CK that have ever been sent are tied to A's and B's secret keys. B is in a similar state, mutatis mutandis. It is important, however, to be sure that no part of the protocol exchange or ensuing conversation is being replayed by an intruder from a recording of a previous conversation between A and B. In relationship to this question the positions of A and B differ. A is aware that he has not used the key CK before and therefore has

no reason to fear that material encrypted with it is other than the legitimate responses from B. B's position is not so good; unless he remembers indefinitely keys previously used by A in order to check that CK is new, he is unclear that the message (1.3) and the subsequent messages supposedly from A are not being replayed. To guard against this possibility, B generates a nonce identifier for the transaction, I_B, and sends it to A under CK:

B --) A: $\{I_B\}^{CK}$ (1.4)

expecting a related reply, say one less:

A --) B: $\{I_B - 1\}^{CK}$ (1.5)

If this reply is satisfactorily received, then the mutual confidence is sufficient to enable substantive communication, encrypted with CK, to begin.

As to claim 3, the modified Stevens discloses the method of claim 2, wherein the key-exchange protocol corresponds to a Needham-Schroeder key-exchange protocol (Needham page 995, column 1, paragraph 2-4 and column 2, paragraph 1: The protocol opens with A communicating in clear to AS his own claimed identity and the identity of the desired correspondent, B, together with A's nonce identifier for this transaction, I_{a1}. ("Nonce" means "used only once.") Here the nonce identifier must be different than others used by A in previous messages of the same type. The first message of the protocol is:

A --) AS: A, B, I_{Al} (1.1)

Upon receiving message (1.1), AS looks up the secret, identifying keys of both parties and also computes a new key CK that will be the key for the conversation if all goes well. The next transaction is a rather complicated message from A S to A:

AS--) A: $\{I_{A1}, B, CK, \{CK, A\}^{KB}\}^{KA}$ (1.2)

where KA and KB are A's and B's secret, identifying keys. Because (1.2) is encrypted with A's secret key, only A can decrypt it and discover the conversation key CK. Following decryption, A checks for the presence of the intended recipient's name, B, and the correct identifier, I_{A1}, in order to verify that the message really is a reply by AS to the current enquiry. Both the name of the intended recipient and the transaction identifier must appear in message (1.2). If the recipient's name is left out, then an intruder could change that name in message (1.1), say to X, before AS receives it, with the subsequent result that A would unknowingly communicate with X instead of B. If the identifier is left out, then an intruder could substitute a previously recorded message (1.2) (from AS to A about B) and force A to reuse a previous conversation key. A remembers CK and sends the part encrypted with KB to B:

A --) B: $\{CK, A\}^{KB}$ (1.3)

The real B, but no other, will be able to decrypt message (1.3) and emerge with the conversation key CK, the same as A has. B also knows the identity of the intending correspondent, as authenticated by AS.

It is worth reviewing at this point the state of knowledge of the two parties. A now knows that any communication he receives encrypted with CK must have originated with B, and also that any communication he emits with CK encryption will be understood only by B. Both are known because the only messages containing CK that have ever been sent are tied to A's and B's secret keys. B is in a similar state, mutatis mutandis. It is important, however, to be sure that no part of the protocol exchange or ensuing conversation is being replayed by an intruder from a recording of a previous conversation between A and B. In relationship to this question the positions of A and B differ. A is aware that he has not used the key CK before and therefore has

no reason to fear that material encrypted with it is other than the legitimate responses from B. B's position is not so good; unless he remembers indefinitely keys previously used by A in order to check that CK is new, he is unclear that the message (1.3) and the subsequent messages supposedly from A are not being replayed. To guard against this possibility, B generates a nonce identifier for the transaction, I_B, and sends it to A under CK:

B --) A: $\{I_B\}^{CK}$ (1.4)

expecting a related reply, say one less:

A --) B: $\{I_B - 1\}^{CK}$ (1.5)

If this reply is satisfactorily received, then the mutual confidence is sufficient to enable substantive communication, encrypted with CK, to begin.

As to claim 5, the modified Stevens discloses the method of claim 1, wherein the measure of processing time at the target node is predefined (Stevens page 2, paragraph 4: …these newer implementations send only a single echo request and output "host is alive" if an echo reply is received, or "no answer" if no reply is received within 20 seconds).

As to claim 6, the modified Stevens discloses the method of claim 1, wherein determining the proximity includes comparing the communication time to a threshold value that distinguishes between local and remote nodes (Stevens page 2, paragraph 4: …these newer implementations send only a single echo request and output "host is alive" if an echo reply is received, or "no answer" if no reply is received within 20 seconds) (If the reply is less then 20 seconds it could be local).

As to claim 7, the modified Stevens discloses the method of claim 1, further including restricting communications with the target node based on the proximity (Stevens page 2, paragraph 4: ...these newer implementations send only a single echo request and output "host is alive" if an echo reply is received, or "no answer" if no reply is received within 20 seconds) (If the reply is less then 20 seconds it could be local).

As to claim 8, the modified Stevens discloses the method of claim 1. The modified Stevens fails to teach wherein the response is cryptographically signed by the target node.

However, Needham discloses wherein the response is cryptographically signed by the target node (Needham page 998, paragraph 1: ...To produce the analog of signed documents with messages, it is necessary that the recipient could not alter a signed text undetected and that the sender cannot credible disclaim it. The ability to provide digital signatures depends upon there being something the originator can do which the recipient cannot).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that digital signatures can be used to authenticate both target and source (Needham page 998, paragraph 1: ...To produce the analog of signed documents with messages, it is necessary that the recipient could not alter a signed text undetected and that the sender cannot credible disclaim it. The ability to provide digital signatures depends upon there being something the originator can do which the recipient cannot).

As to claim 9, Wang discloses a node on a network including: a communication device that is configured to receive a query from a source node and to transmit a corresponding response to the source node, a processor that is configured to process the query and produce therefrom the response (Wang Figure 6), wherein the response includes a measure of processing time required to process the query and produce the response (Wang Figure 5).

As to claim 10, Wang discloses the node of claim 9. Wang fails to teach wherein the processor is configured to process the query and produce the response as part of a cryptographic key-exchange protocol.

However, Needham discloses wherein the processor is configured to process the query and produce the response as part of a cryptographic key-exchange protocol (Needham page 995, column 1, paragraph 2-4 and column 2, paragraph 1: The protocol opens with A communicating in clear to AS his own claimed identity and the identity of the desired correspondent, B, together with A's nonce identifier for this transaction, I_{a1}. ("Nonce" means "used only once.") Here the nonce identifier must be different than others used by A in previous messages of the same type. The first message of the protocol is:

A --) AS: A, B, I_{A1} (1.1)

Upon receiving message (1.1), AS looks up the secret, identifying keys of both parties and also computes a new key CK that will be the key for the conversation if all goes well. The next transaction is a rather complicated message from A S to A:

AS--) A: $\{I_{A1}, B, CK, \{CK, A\}^{KB}\}^{KA}$ (1.2)

where KA and KB are A's and B's secret, identifying keys. Because (1.2) is encrypted with A's secret key, only A can decrypt it and discover the conversation key CK. Following decryption, A checks for the presence of the intended recipient's name, B, and the correct identifier, I_{A1}, in order to verify that the message really is a reply by AS to the current enquiry. Both the name of the intended recipient and the transaction identifier must appear in message (1.2). If the recipient's name is left out, then an intruder could change that name in message (1.1), say to X, before AS receives it, with the subsequent result that A would unknowingly communicate with X

instead of B. If the identifier is left out, then an intruder could substitute a previously recorded message (1.2) (from AS to A about B) and force A to reuse a previous conversation key. A remembers CK and sends the part encrypted with KB to B:

A --) B: $\{CK, A\}^{KB}$ (1.3)

The real B, but no other, will be able to decrypt message (1.3) and emerge with the conversation key CK, the same as A has. B also knows the identity of the intending correspondent, as authenticated by AS.

It is worth reviewing at this point the state of knowledge of the two parties. A now knows that any communication he receives encrypted with CK must have originated with B, and also that any communication he emits with CK encryption will be understood only by B. Both are known because the only messages containing CK that have ever been sent are tied to A's and B's secret keys. B is in a similar state, mutatis mutandis. It is important, however, to be sure that no part of the protocol exchange or ensuing conversation is being replayed by an intruder from a recording of a previous conversation between A and B. In relationship to this question the positions of A and B differ. A is aware that he has not used the key CK before and therefore has no reason to fear that material encrypted with it is other than the legitimate responses from B. B's position is not so good; unless he remembers indefinitely keys previously used by A in order to check that CK is new, he is unclear that the message (1.3) and the subsequent messages supposedly from A are not being replayed. To guard against this possibility, B generates a nonce identifier for the transaction, I_B, and sends it to A under CK:

B --) A: $\{I_B\}^{CK}$ (1.4)

expecting a related reply, say one less:

A --) B: $\{I_B - 1\}^{CK}$ (1.5)

If this reply is satisfactorily received, then the mutual confidence is sufficient to enable substantive communication, encrypted with CK, to begin.

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that this Needham-Schroeder key-exchange protocol is a cryptographic key-exchange protocol (Needham page 995, column 1, paragraph 2-4 and column 2, paragraph 1: The protocol opens with A communicating in clear to AS his own claimed identity and the identity of the desired correspondent, B, together with A's nonce identifier for this transaction, I_{a1}. ("Nonce" means "used only once.") Here the nonce identifier must be different than others used by A in previous messages of the same type. The first message of the protocol is:

A --) AS: A, B, I_{AI}· (1.1)

Upon receiving message (1.1), AS looks up the secret, identifying keys of both parties and also computes a new key CK that will be the key for the conversation if all goes well. The next transaction is a rather complicated message from A S to A:

AS--) A: $\{I_{A1}, B, CK, \{CK, A\}^{KB}\}^{KA}$ (1.2)

where KA and KB are A's and B's secret, identifying keys. Because (1.2) is encrypted with A's secret key, only A can decrypt it and discover the conversation key CK. Following decryption, A checks for the presence of the intended recipient's name, B, and the correct identifier, I_{A1}, in order to verify that the message really is a reply by AS to the current enquiry. Both the name of the intended recipient and the transaction identifier must appear in message (1.2). If the recipient's name is left out, then an intruder could change that name in message (1.1), say to X, before AS receives it, with the subsequent result that A would unknowingly communicate with X

instead of B. If the identifier is left out, then an intruder could substitute a previously recorded message (1.2) (from AS to A about B) and force A to reuse a previous conversation key. A remembers CK and sends the part encrypted with KB to B:

A --) B: $\{CK, A\}^{KB}$ (1.3)

The real B, but no other, will be able to decrypt message (1.3) and emerge with the conversation key CK, the same as A has. B also knows the identity of the intending correspondent, as authenticated by AS.

It is worth reviewing at this point the state of knowledge of the two parties. A now knows that any communication he receives encrypted with CK must have originated with B, and also that any communication he emits with CK encryption will be understood only by B. Both are known because the only messages containing CK that have ever been sent are tied to A's and B's secret keys. B is in a similar state, mutatis mutandis. It is important, however, to be sure that no part of the protocol exchange or ensuing conversation is being replayed by an intruder from a recording of a previous conversation between A and B. In relationship to this question the positions of A and B differ. A is aware that he has not used the key CK before and therefore has no reason to fear that material encrypted with it is other than the legitimate responses from B. B's position is not so good; unless he remembers indefinitely keys previously used by A in order to check that CK is new, he is unclear that the message (1.3) and the subsequent messages supposedly from A are not being replayed. To guard against this possibility, B generates a nonce identifier for the transaction, I_B, and sends it to A under CK:

B --) A: $\{I_B\}^{CK}$ (1.4)

expecting a related reply, say one less:

A --) B: $\{I_B - 1\}^{CK}$ (1.5)

If this reply is satisfactorily received, then the mutual confidence is sufficient to enable substantive communication, encrypted with CK, to begin.

As to claim 11, the modified Wang discloses the node of claim 10, wherein the key-exchange protocol corresponds to a Needham-Schroeder key-exchange protocol (Needham page 995, column 1, paragraph 2-4 and column 2, paragraph 1: The protocol opens with A communicating in clear to AS his own claimed identity and the identity of the desired correspondent, B, together with A's nonce identifier for this transaction, I_{a1}. ("Nonce" means "used only once.") Here the nonce identifier must be different than others used by A in previous messages of the same type. The first message of the protocol is:

A --) AS: A, B, I_{A1} (1.1)

Upon receiving message (1.1), AS looks up the secret, identifying keys of both parties and also computes a new key CK that will be the key for the conversation if all goes well. The next transaction is a rather complicated message from A S to A:

AS--) A: $\{I_{A1}, B, CK, \{CK, A\}^{KB}\}^{KA}$ (1.2)

where KA and KB are A's and B's secret, identifying keys. Because (1.2) is encrypted with A's secret key, only A can decrypt it and discover the conversation key CK. Following decryption, A checks for the presence of the intended recipient's name, B, and the correct identifier, I_{A1}, in order to verify that the message really is a reply by AS to the current enquiry. Both the name of the intended recipient and the transaction identifier must appear in message (1.2). If the recipient's name is left out, then an intruder could change that name in message (1.1), say to X, before AS receives it, with the subsequent result that A would unknowingly communicate with X

instead of B. If the identifier is left out, then an intruder could substitute a previously recorded message (1.2) (from AS to A about B) and force A to reuse a previous conversation key. A remembers CK and sends the part encrypted with KB to B:

A --) B: $\{CK, A\}^{KB}$ (1.3)

The real B, but no other, will be able to decrypt message (1.3) and emerge with the conversation key CK, the same as A has. B also knows the identity of the intending correspondent, as authenticated by AS.

It is worth reviewing at this point the state of knowledge of the two parties. A now knows that any communication he receives encrypted with CK must have originated with B, and also that any communication he emits with CK encryption will be understood only by B. Both are known because the only messages containing CK that have ever been sent are tied to A's and B's secret keys. B is in a similar state, mutatis mutandis. It is important, however, to be sure that no part of the protocol exchange or ensuing conversation is being replayed by an intruder from a recording of a previous conversation between A and B. In relationship to this question the positions of A and B differ. A is aware that he has not used the key CK before and therefore has no reason to fear that material encrypted with it is other than the legitimate responses from B. B's position is not so good; unless he remembers indefinitely keys previously used by A in order to check that CK is new, he is unclear that the message (1.3) and the subsequent messages supposedly from A are not being replayed. To guard against this possibility, B generates a nonce identifier for the transaction, I_B, and sends it to A under CK:

B --) A: $\{I_B\}^{CK}$ (1.4)

expecting a related reply, say one less:

A --) B: $\{I_B - 1\}^{CK}$ (1.5)

If this reply is satisfactorily received, then the mutual confidence is sufficient to enable substantive communication, encrypted with CK, to begin.

As to claim 13, Wang discloses the node of claim 9. Wang fails to teach wherein the measure of processing time is predefined.

However, Stevens discloses wherein the measure of processing time is predefined (Stevens page 2, paragraph 4: ...these newer implementations send only a single echo request and output "host is alive" if an echo reply is received, or "no answer" if no reply is received within 20 seconds).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Wang and Stevens because Wang gives more details for the monitoring and calculating then Stevens does (Stevens page 2, paragraph 4: ...these newer implementations send only a single echo request and output "host is alive" if an echo reply is received, or "no answer" if no reply is received within 20 seconds).

As to claim 14, Wang discloses the node of claim 9. Wang fails to teach wherein the processor is further configured to cryptographically sign the response.

However, Needham discloses wherein the processor is further configured to cryptographically sign the response (Needham page 998, paragraph 1: ...To produce the analog of signed documents with messages, it is necessary that the recipient could not alter a signed text undetected and that the sender cannot credible disclaim it. The ability to provide digital signatures depends upon there being something the originator can do which the recipient cannot).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that digital signatures can be used to authenticate both target and source (Needham page 998, paragraph 1: ...To produce the analog of signed documents with messages, it is necessary that the recipient could not alter a signed text undetected and that the sender cannot credible disclaim it. The ability to provide digital signatures depends upon there being something the originator can do which the recipient cannot).

As to claim 15, Wang discloses a node on a network including: a communication device that is configured to transmit a query to a target node and to receive a corresponding response from the target node, the response from the target node including a measure of processing time required to generate the response at the target node, and a processor that is configured to: generate the query, receive the response, measure a query-response time between generating the query and receiving the response (Wang abstract: A client-server software performance monitor system is disclosed. In the system of the present invention, a performance monitor machine is coupled to a computer network in close network proximity to one or more server systems that are to be monitored. The performance monitor machine monitors all network communication originating from or addressed to the server system to determine client-server transaction times. The performance monitor machine calculates a server processing time by subtracting the time when the server system receives the request packet from a client system from the time when the server system sends the first response packet back to the client system. The performance monitor machine also calculates an network transit time by subtracting said time when the server system receives the final acknowledgement packet from the time when said server system sent the first response packet to the client system. The performance monitor machine calculates an approximate total client observed response time by adding the server processing time and the approximate network transit time). Wang fails to teach and determine a proximity of the target node relative to the node based on a communication time that is dependent upon a difference between the query-response time and the measure of processing time.

However, Stevens discloses and determine a proximity of the target node relative to the node based on a communication time that is dependent upon a difference between the query-response time and the measure of processing time (Stevens page 2, paragraph 4: ...these newer implementations send only a single echo request and output "host is alive" if an echo reply is received, or "no answer" if no reply is received within 20 seconds).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention because Wang calculates the details whereas Stevens just says "calculate", so Wang fills in those details (Stevens page 2, paragraph 4: ...these newer implementations send only a single echo request and output "host is alive" if an echo reply is received, or "no answer" if no reply is received within 20 seconds).

As to claim 16, the modified Wang discloses the node of claim 15. The modified Wang fails to teach wherein the processor is configured to generate the query and receive the response as part of a cryptographic key-exchange protocol.

However, Needham discloses wherein the processor is configured to generate the query and receive the response as part of a cryptographic key-exchange protocol (Needham page 995, column 1, paragraph 2-4 and column 2, paragraph 1: The protocol opens with A communicating in clear to AS his own claimed identity and the identity of the desired correspondent, B, together with A's nonce identifier for this transaction, I_{a1}. ("Nonce" means "used only once.") Here the nonce identifier must be different than others used by A in previous messages of the same type. The first message of the protocol is:

A --) AS: A, B, I_{AI} (1.1)

Upon receiving message (1.1), AS looks up the secret, identifying keys of both parties and also computes a new key CK that will be the key for the conversation if all goes well. The next transaction is a rather complicated message from A S to A:

AS--) A: $\{I_{A1}, B, CK, \{CK, A\}^{KB}\}^{KA}$ (1.2)

where KA and KB are A's and B's secret, identifying keys. Because (1.2) is encrypted with A's secret key, only A can decrypt it and discover the conversation key CK. Following decryption, A checks for the presence of the intended recipient's name, B, and the correct identifier, I_{A1}, in order to verify that the message really is a reply by AS to the current enquiry. Both the name of the intended recipient and the transaction identifier must appear in message (1.2). If the recipient's name is left out, then an intruder could change that name in message (1.1), say to X, before AS receives it, with the subsequent result that A would unknowingly communicate with X instead of B. If the identifier is left out, then an intruder could substitute a previously recorded message (1.2) (from AS to A about B) and force A to reuse a previous conversation key. A remembers CK and sends the part encrypted with KB to B:

A --) B: $\{CK, A\}^{KB}$ (1.3)

The real B, but no other, will be able to decrypt message (1.3) and emerge with the conversation key CK, the same as A has. B also knows the identity of the intending correspondent, as authenticated by AS.

It is worth reviewing at this point the state of knowledge of the two parties. A now knows that any communication he receives encrypted with CK must have originated with B, and also that any communication he emits with CK encryption will be understood only by B. Both are known because the only messages containing CK that have ever been sent are tied to A's and B's secret keys. B is in a similar state, mutatis mutandis. It is important, however, to be sure that no part of the protocol exchange or ensuing conversation is being replayed by an intruder from a recording of a previous conversation between A and B. In relationship to this question the positions of A and B differ. A is aware that he has not used the key CK before and therefore has no reason to fear that material encrypted with it is other than the legitimate responses from B. B's position is not so good; unless he remembers indefinitely keys previously used by A in order to check that CK is new, he is unclear that the message (1.3) and the subsequent messages supposedly from A are not being replayed. To guard against this possibility, B generates a nonce identifier for the transaction, I_B, and sends it to A under CK:

B --) A: $\{I_B\}^{CK}$ (1.4)

expecting a related reply, say one less:

A --) B: $\{I_B - 1\}^{CK}$ (1.5)

If this reply is satisfactorily received, then the mutual confidence is sufficient to enable substantive communication, encrypted with CK, to begin.

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that this Needham-Schroeder key-exchange protocol is a cryptographic key-exchange protocol (Needham page 995, column 1, paragraph 2-4 and column 2, paragraph 1: The protocol opens with A communicating in clear to AS his own claimed identity and the identity of the desired correspondent, B, together with A's nonce identifier for this transaction, I_{a1}. ("Nonce" means "used only once.") Here the nonce identifier must be different than others used by A in previous messages of the same type. The first message of the protocol is:

A --) AS: A, B, I_{AI} (1.1)

Upon receiving message (1.1), AS looks up the secret, identifying keys of both parties and also computes a new key CK that will be the key for the conversation if all goes well. The next transaction is a rather complicated message from A S to A:

AS--) A: $\{I_{A1}, B, CK, \{CK, A\}^{KB}\}^{KA}$ (1.2)

where KA and KB are A's and B's secret, identifying keys. Because (1.2) is encrypted with A's secret key, only A can decrypt it and discover the conversation key CK. Following decryption, A checks for the presence of the intended recipient's name, B, and the correct identifier, I_{A1}, in order to verify that the message really is a reply by AS to the current enquiry. Both the name of the intended recipient and the transaction identifier must appear in message (1.2). If the recipient's name is left out, then an intruder could change that name in message (1.1), say to X, before AS receives it, with the subsequent result that A would unknowingly communicate with X instead of B. If the identifier is left out, then an intruder could substitute a previously recorded message (1.2) (from AS to A about B) and force A to reuse a previous conversation key. A remembers CK and sends the part encrypted with KB to B:

A --) B: $\{CK, A\}^{KB}$ (1.3)

The real B, but no other, will be able to decrypt message (1.3) and emerge with the conversation key CK, the same as A has. B also knows the identity of the intending correspondent, as authenticated by AS.

It is worth reviewing at this point the state of knowledge of the two parties. A now knows that any communication he receives encrypted with CK must have originated with B, and also that any communication he emits with CK encryption will be understood only by B. Both are known because the only messages containing CK that have ever been sent are tied to A's and B's secret keys. B is in a similar state, mutatis mutandis. It is important, however, to be sure that no part of the protocol exchange or ensuing conversation is being replayed by an intruder from a recording of a previous conversation between A and B. In relationship to this question the positions of A and B differ. A is aware that he has not used the key CK before and therefore has no reason to fear that material encrypted with it is other than the legitimate responses from B. B's position is not so good; unless he remembers indefinitely keys previously used by A in order to check that CK is new, he is unclear that the message (1.3) and the subsequent messages supposedly from A are not being replayed. To guard against this possibility, B generates a nonce identifier for the transaction, I_B, and sends it to A under CK:

B --) A: $\{I_B\}^{CK}$ (1.4)

expecting a related reply, say one less:

A --) B: $\{I_B - 1\}^{CK}$ (1.5)

If this reply is satisfactorily received, then the mutual confidence is sufficient to enable substantive communication, encrypted with CK, to begin.

As to claim 17, the modified Wang discloses the node of claim 16, wherein the key-exchange protocol corresponds to a Needham-Schroeder key-exchange protocol (Needham page 995, column 1, paragraph 2-4 and column 2, paragraph 1: The protocol opens with A communicating in clear to AS his own claimed identity and the identity of the desired correspondent, B, together with A's nonce identifier for this transaction, I_{a1}. ("Nonce" means "used only once.") Here the nonce identifier must be different than others used by A in previous messages of the same type. The first message of the protocol is:

A --) AS: A, B, I_{A1} (1.1)

Upon receiving message (1.1), AS looks up the secret, identifying keys of both parties and also computes a new key CK that will be the key for the conversation if all goes well. The next transaction is a rather complicated message from A S to A:

AS--) A: $\{I_{A1}, B, CK, \{CK, A\}^{KB}\}^{KA}$ (1.2)

where KA and KB are A's and B's secret, identifying keys. Because (1.2) is encrypted with A's secret key, only A can decrypt it and discover the conversation key CK. Following decryption, A checks for the presence of the intended recipient's name, B, and the correct identifier, I_{A1}, in order to verify that the message really is a reply by AS to the current enquiry. Both the name of the intended recipient and the transaction identifier must appear in message (1.2). If the recipient's name is left out, then an intruder could change that name in message (1.1), say to X, before AS receives it, with the subsequent result that A would unknowingly communicate with X instead of B. If the identifier is left out, then an intruder could substitute a previously recorded message (1.2) (from AS to A about B) and force A to reuse a previous conversation key. A remembers CK and sends the part encrypted with KB to B:

A --) B: $\{CK, A\}^{KB}$ (1.3)

The real B, but no other, will be able to decrypt message (1.3) and emerge with the conversation key CK, the same as A has. B also knows the identity of the intending correspondent, as authenticated by AS.

It is worth reviewing at this point the state of knowledge of the two parties. A now knows that any communication he receives encrypted with CK must have originated with B, and also that any communication he emits with CK encryption will be understood only by B. Both are known because the only messages containing CK that have ever been sent are tied to A's and B's secret keys. B is in a similar state, mutatis mutandis. It is important, however, to be sure that no part of the protocol exchange or ensuing conversation is being replayed by an intruder from a recording of a previous conversation between A and B. In relationship to this question the positions of A and B differ. A is aware that he has not used the key CK before and therefore has no reason to fear that material encrypted with it is other than the legitimate responses from B. B's position is not so good; unless he remembers indefinitely keys previously used by A in order to check that CK is new, he is unclear that the message (1.3) and the subsequent messages supposedly from A are not being replayed. To guard against this possibility, B generates a nonce identifier for the transaction, I_B, and sends it to A under CK:

B --) A: $\{I_B\}^{CK}$ (1.4)

expecting a related reply, say one less:

A --) B: $\{I_B - 1\}^{CK}$ (1.5)

If this reply is satisfactorily received, then the mutual confidence is sufficient to enable substantive communication, encrypted with CK, to begin.

As to claim 19, the modified Wang discloses the node of claim 15. The modified Wang fails to teach wherein the measure of processing time is predefined.

However, Stevens discloses wherein the measure of processing time is predefined (Stevens page 2, paragraph 4: ...these newer implementations send only a single echo request and output "host is alive" if an echo reply is received, or "no answer" if no reply is received within 20 seconds).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the modified Wang and Stevens because the modified Wang gives more details for the monitoring and calculating then Stevens does (Stevens page 2, paragraph 4: ...these newer implementations send only a single echo request and output "host is alive" if an echo reply is received, or "no answer" if no reply is received within 20 seconds).

As to claim 20, the modified Wang discloses the node of claim 15. The modified Wang fails to disclose wherein the processor is configured to determine the proximity based on a comparison of the communication time to a threshold value that distinguishes between local and remote nodes.

However, Stevens discloses wherein the processor is configured to determine the proximity based on a comparison of the communication time to a threshold value that distinguishes between local and remote nodes (Stevens page 2, paragraph 4: ...these newer implementations send only a single echo request and output "host is alive" if an echo reply is received, or "no answer" if no reply is received within 20 seconds) (If the reply is less then 20 seconds it could be local).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the modified Wang and Stevens because the modified Wang gives more details for the monitoring and calculating then Stevens does (Stevens page 2, paragraph 4: ...these newer implementations send only a single echo request and output "host is alive" if an echo reply is received, or "no answer" if no reply is received within 20 seconds).

As to claim 21, the modified Wang discloses the node of claim 15. The modified Wang fails to teach wherein the processor is further configured to control subsequent communications with the target node based on the proximity.

However, Stevens discloses wherein the processor is further configured to control subsequent communications with the target node based on the proximity (Stevens page 2, paragraph 4: ...these newer implementations send only a single echo request and output "host is alive" if an echo reply is received, or "no answer" if no reply is received within 20 seconds) (If the reply is less then 20 seconds it could be local).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that Stevens waiting for a reply, and if no answer occurs in 20 seconds, timing out is a way to control the communications with the target node based on its proximity (Stevens page 2, paragraph 4: ...these newer implementations send only a single echo request and output "host is alive" if an echo reply is received, or "no answer" if no reply is received within 20 seconds).

Allowable Subject Matter

8. **Claims 4, 12, and 18 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.**

The following is a statement of reasons for the indication of allowable subject matter: the applicant requires the use of the OCPS protocol in these limitations. This protocol was authored by the applicant less then one year from the filing date of this application.

Prior Art

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. US 6223286 is pertinent because it teaches a multicast message transmission device and a message receiving protocol device for guaranteeing a fair message delivery time for a multicast message. At the receiving protocol device, a release time of the received multicast message is set to a prescribed time specified to all receiving protocol devices of the same multicast group, and the received multicast message is stored until the release time, and then released to a corresponding upper level device. At the transmission device, each receiving protocol device is authenticated, and then the encrypted multicast messages are transmitted to the receiving protocol devices, while a prescribed decryption key corresponding to the encryption key of the encrypted multicast message is distributed the authenticated receiving protocol devices prior to transmissions of the multicast messages. US 6363477 is pertinent because it teaches … where the computer systems are executing network applications that send and receive either encrypted or unencrypted data packets over the communication network, a method for quantifying performance of the communication network. US 6367018 is pertinent because it teaches … The network device then determines whether the end station participates in the test prior to proceeding with the authentication/identification processes. US 7036010 is pertinent because it teaches … A security protocol entity (20) is provided that includes a mechanism for enabling a first party (11) to communicate securely with a second party (60) through an access-controlling intermediate party…

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Rebecca L. Pachura whose telephone number is (571) 270-3402. The examiner can normally be reached on Monday-Thursday 7:30 am-6:00 pm est.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Rebecca L Pachura/
/R. L. P./
Examiner, Art Unit 2136

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

2/6/08